Mission: Continuity

BUILDING RESILIENCE AGAINST UNPLANNED SERVICE INTERRUPTIONS

Stephanie Poe, DNP, RN-BC
CNIO, The Johns Hopkins Hospital and Health System

Discussion Topics

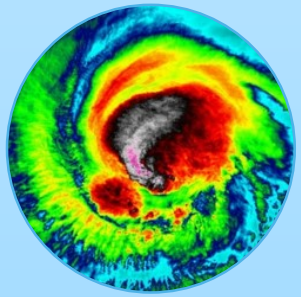
- The "Age of Acceleration"
- Cyber Risk and Cyber Resilience
- Cybersecurity Infrastructure and Nursing Informatics
- Building Cyber Resilience
- Resilience Training Content

The Age of Acceleration

SETTING THE CONTEXT

The Age of Acceleration

Exponential Growth of Computing Power (Technology)



Compelling Evidence of Climate Change

Massive Globalization

Cyber Risk
as defined by the Institute of Risk Management

- Any risk of financial loss, service disruption, or reputational damage to an organization from some sort of failure of its information technology systems.

Not a question of “if”, but “when”

An Emerging Lexicon

- Cyberattack
- Cyber Crime
- Cyber Ecosystem
- Cyber Event
- Cyber Exercise
- Cyber Health/Safety
- Cyber Hygiene
- Cyber Incident
- Cyber Infrastructure
- Cyber Literacy
- Cyber Operations
- Cyber Ops Planning
- Cyber Risk
- **Cybersecurity**
- Cyber Threat
- **Cyber Resilience**

Data Breach

Hacktivism

Phishing

Ransomware

Social Engineering

Massive Security Flaws

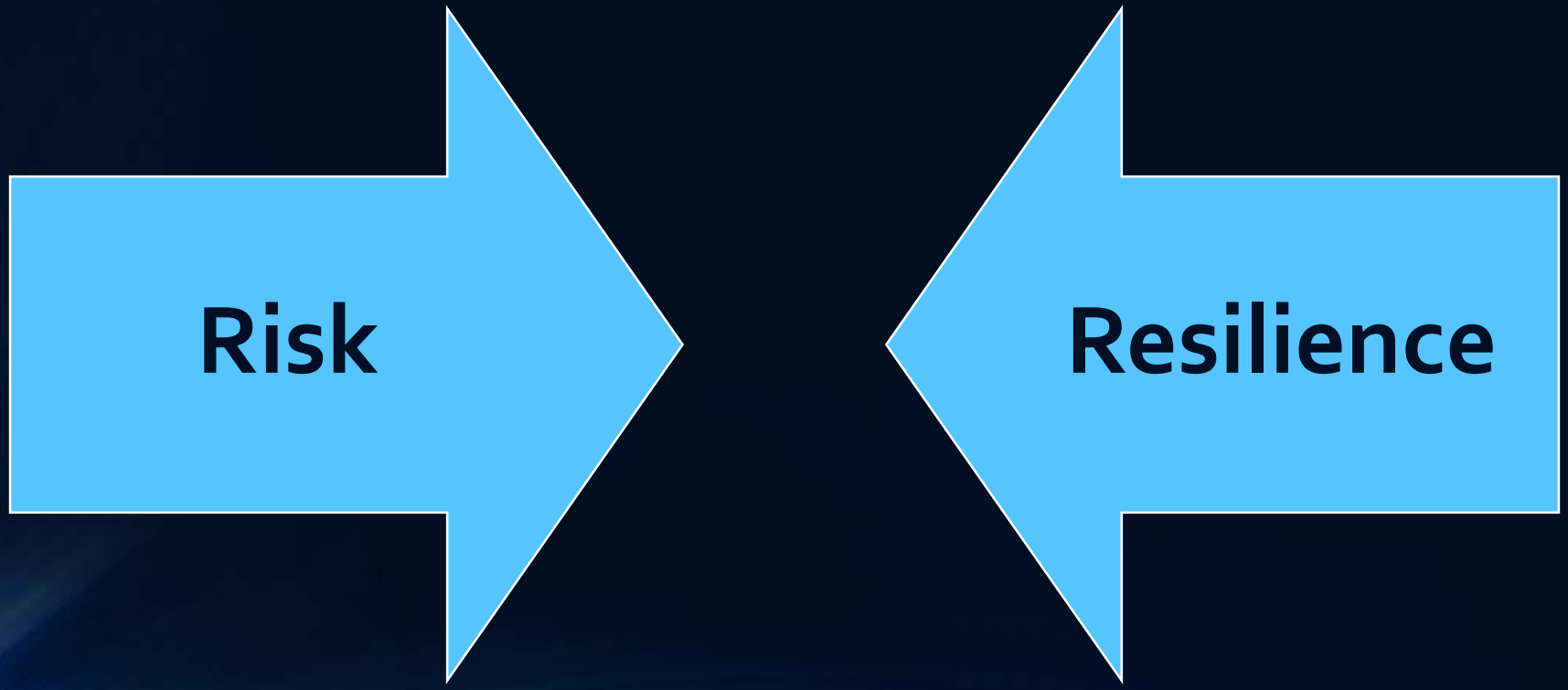
Cyber Risk Threatens

- HIPAA security
- Personal security
- Business continuity
- Service excellence
- Patient safety
- Financial stability

Cyber Resilience

CRITICAL CYBERSECURITY INFRASTRUCTURE AND THE ROLE OF NURSING INFORMATICS SPECIALISTS

Given the inevitability of cyber incidents, how can we best prepare?



Cybersecurity

Systemic challenge

Affects digital economy & society

Risk is loss of networks, data, services

Risk is reputational and existential

Urgency is "now"

World Economic Forum (2017). System Initiative on the Digital Economy and Society: Advancing Cyber Resilience: Principles and tools for Boards.

NIST Definitions

- Cybersecurity: process of protecting information by preventing, detecting, and responding to attacks
- Cyber Event: change that may have an impact on organizational operations
- Cyber Incident: event that has been determined to have an impact on the organization prompting the need for response and recovery

Critical Infrastructure Components

Identify	Asset management
	Business environment
	Governance
	Risk assessment
	Risk mitigation
	Supply chain risk management

NIST Framework for Improving Critical Infrastructure Cybersecurity, 2018

Partnership for Identify Function

Emergency Management

Clinical Informatics

Information Technology

Critical Infrastructure Components

Protect	Identity management
	Authentication
	Access control
	Cybersecurity awareness and training
	Data security
	Information protection processes
	Maintenance and repairs
	Protective technology

NIST Framework for Improving Critical Infrastructure Cybersecurity, 2018

Partnership for Protect Function

Access Security

Academic Trainees

Cybersecurity Training

Critical Infrastructure Components

Detect

- Anomalies and events
- Security continuum monitoring
- Detection processes

NIST Framework for Improving Critical Infrastructure Cybersecurity, 2018

Partnership for Detect Function

High Reliability

Situational Awareness

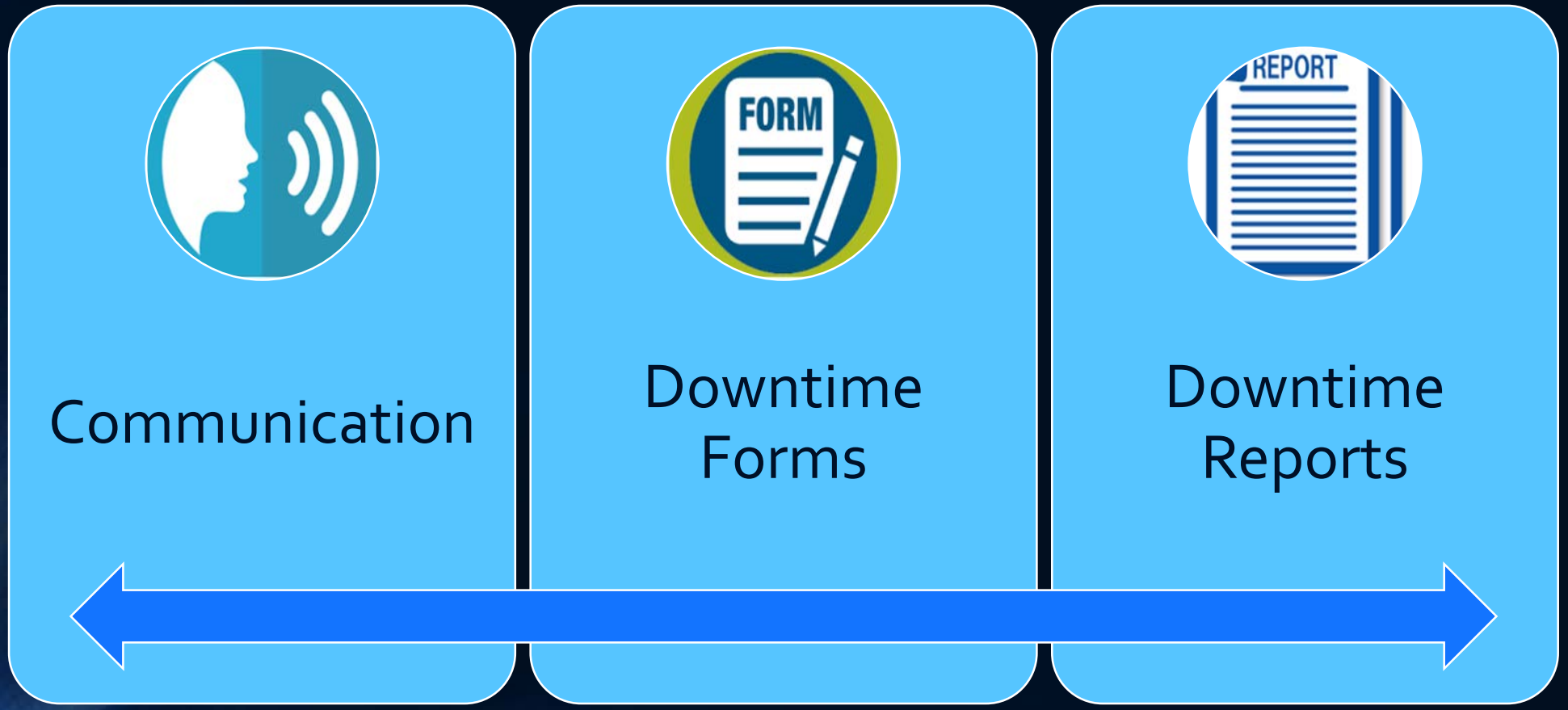
Vigilance Training

Critical Infrastructure Components

Respond	Response planning
	Communication
	Analysis
	Mitigation
	Improvements

NIST Framework for Improving Critical Infrastructure Cybersecurity, 2018

Partnership for Respond Function



Critical Infrastructure Components

Recover	Recovery planning
	Communication

NIST Framework for Improving Critical Infrastructure Cybersecurity, 2018

Partnership for Recovery Function

Recovery Procedures

Short-term Recovery

Long-term Recovery

Building Cyber Resilience

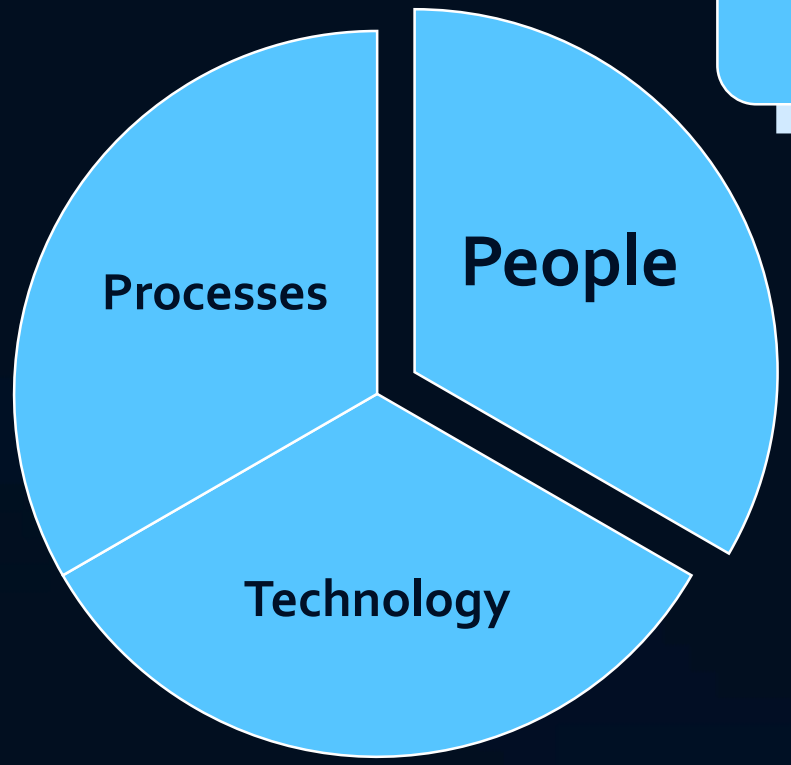
STOP – THINK - CONNECT

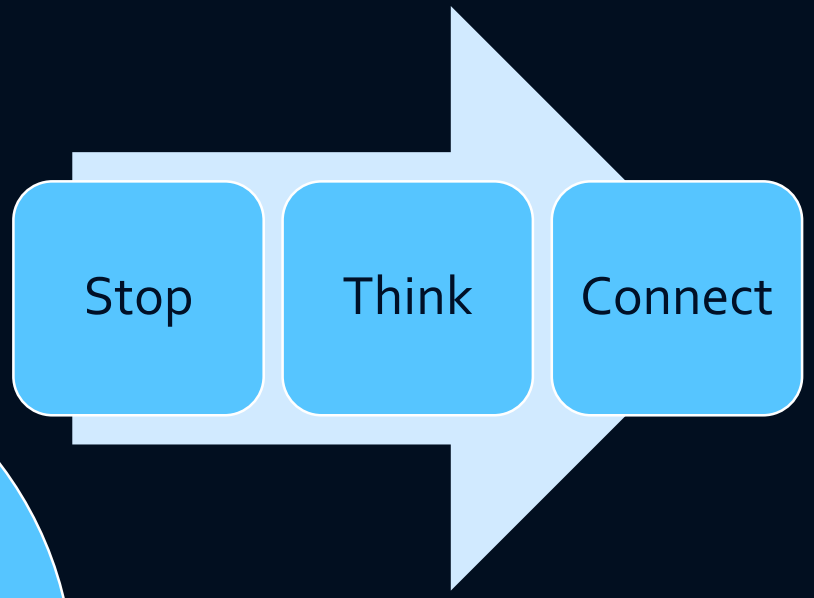
Cyber-Resilience

- A public good
- Information stewardship
- Strategy & culture versus tactics
- Accountability: Board and Executive Team
- Responsibility: All

World Economic Forum (2017). System Initiative on the Digital Economy and Society: Advancing Cyber Resilience: Principles and tools for Boards.

Cybersecurity Triad



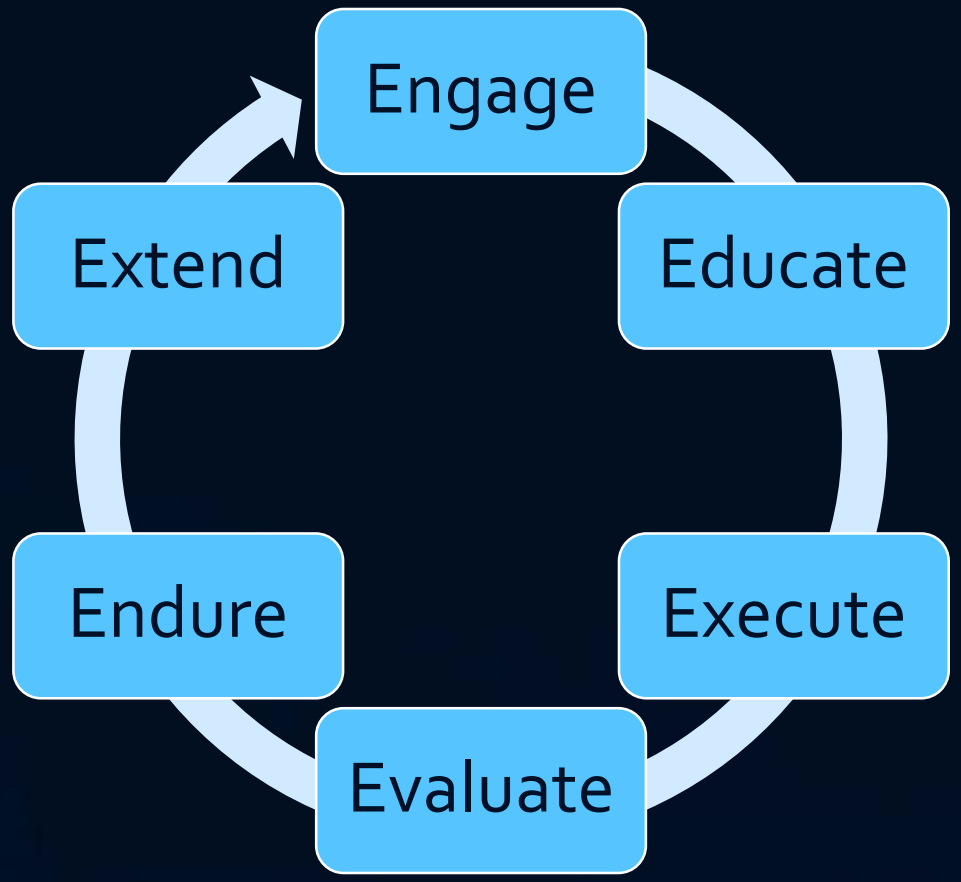


National Cybersecurity Awareness Month – every October: collaborative effort between government and industry

Staff Awareness

- Password Safety?
- Phishing?
- Reporting suspicious activity?
- Social media?
- BYOD?
- Connected medical devices?
- Removable data?
- Personal information?
- Information handling?
- Remote and mobile working?
- Web plug-ins?
- Shadow IT or free software?

Developing Cyber Resilience in Faculty and Employees



Johns Hopkins Research & Quality Group Translation Model, Pronovost et. al., 2008

Developing Resilience

Engage

- Who are your stakeholders?
- Know where they stand – their knowledge, their skills
- Make personal connections with real world application
- Promote interest and curiosity

Developing Resilience

Educate

- Where are the knowledge gaps?
- Raise awareness
- Provide information and make it personal
- Encourage inquiry and exploration

Developing Resilience

Execute

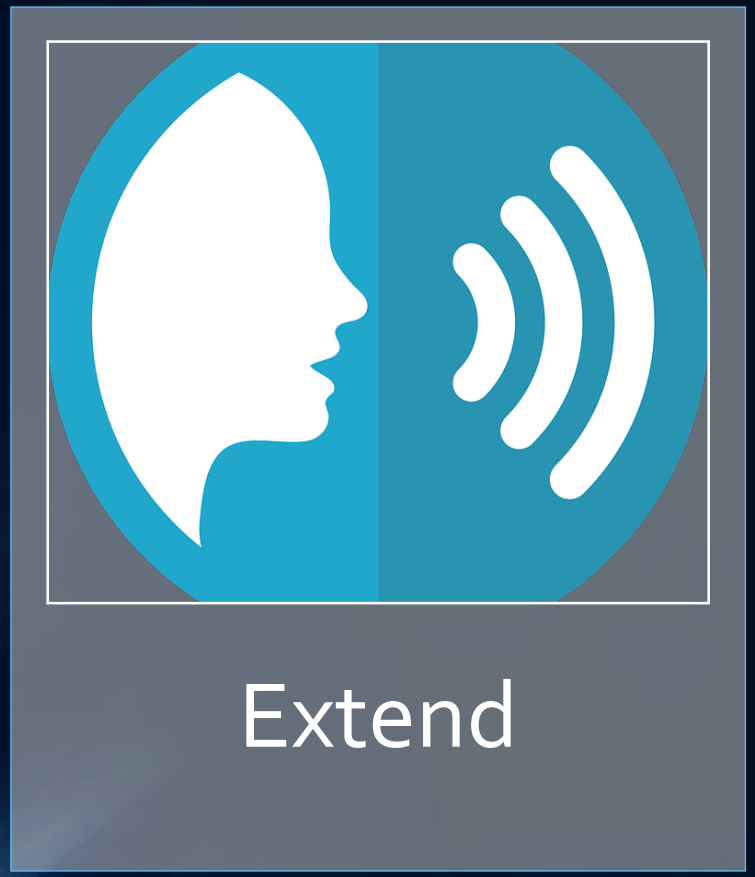
- Assign personal responsibility
- Teach cyber hygiene best practices
- Test cyber hygiene competency
- Practice IT emergency management

Developing Resilience

Evaluate

- Monitor behaviors
- Review incident reports related to security breaches
- Debrief unplanned technology outages

Developing Resilience



- Share best practices across job roles
- Share lessons learned during unplanned outages
- Design for high reliability

Developing Resilience

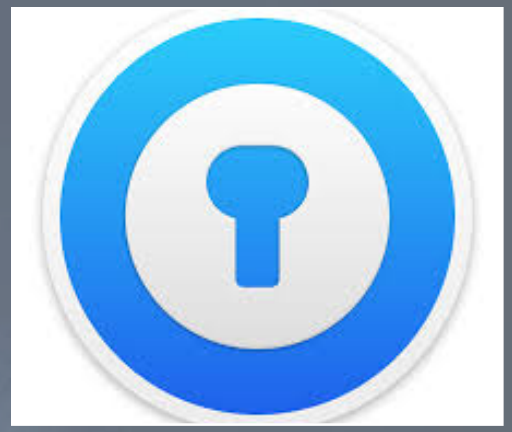
Endure

- Plan for sustaining resilience over time
- Conduct refreshers
- Hold cyber hygiene campaigns
- Reward/recognize resilience behaviors

Sample Educational Content

HARDWIRING CYBER HYGIENE PRACTICES TO BUILD RESILIENCE

Teaching Principles of Good Cyber Hygiene

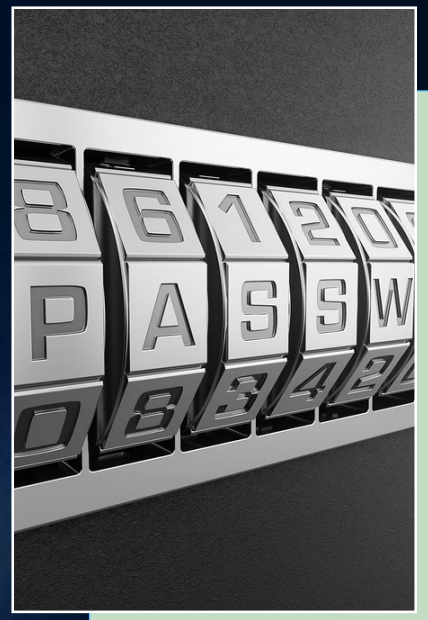


Password management

Situational awareness

Phishing detection

Cyber Hygiene Best Practices – for end users



Use $trOng3r passwords (use numbers, symbols, upper & lower case letters)

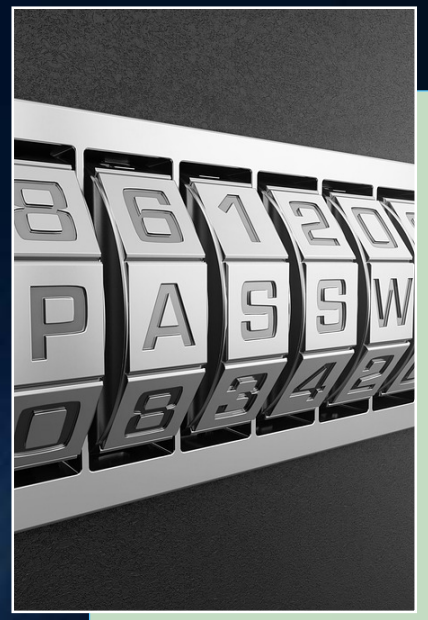
Cyber Hygiene Best Practices – for end users

Change passwords regularly (every 45-90 days)

Cyber Hygiene Best Practices – for end users

Don’t change your passwords or enter personal credentials over public Wi-Fi

Cyber Hygiene Best Practices – for end users



Don’t share usernames, passwords, or access codes with anyone

Cyber Hygiene Best Practices – for end users

Don’t open emails, links, or attachments from strangers

Cyber Hygiene Best Practices – for end users

Disable Auto connect Wi-Fi or enable "Ask to Join Networks"

Cyber Hygiene Best Practices – for end users

Use your cell network when security is important (4G, 5G, LTE)

Cyber Hygiene Best Practices – for end users

Limit personally identifiable information on social media

Cyber Hygiene Best Practices – for end users

Limit how often you "like" a status, follow a page, or allow an app to access your social media profile

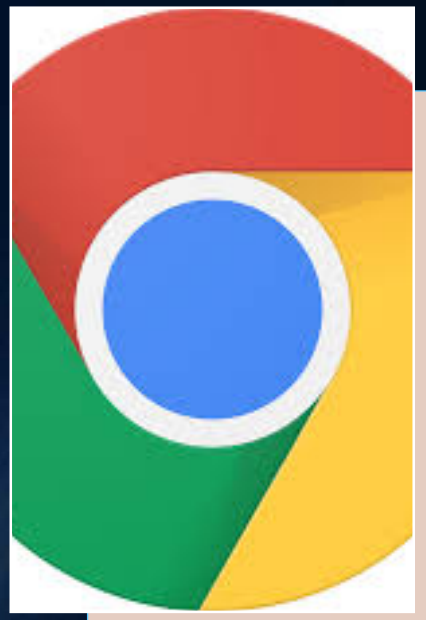
Cyber Hygiene Best Practices – for end users

Be wary of unsolicited calls asking you to break normal security features,

Cyber Hygiene Best Practices – for end users

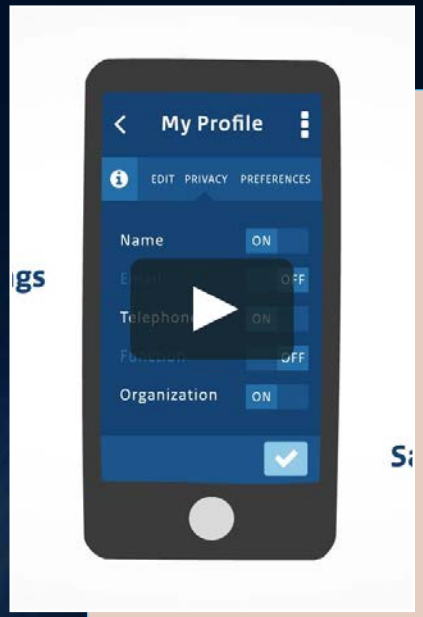
Update apps and computers within 24 hours of notification

Cyber Hygiene Best Practices – for end users



Use the latest browsers; they have improved security

Cyber Hygiene Best Practices – for end users



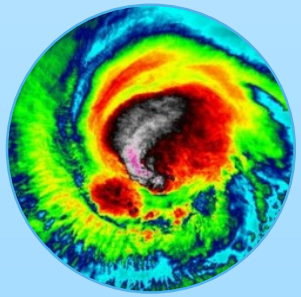
Enable privacy settings, increase default security settings, set up alerts

Cyber Hygiene Best Practices – for end users

Before clicking on anything, stop, think, and check if it is expected, valid & trusted.

Managing The Age of Acceleration

Exponential Growth of Computing Power (Technology)



Compelling Evidence of Climate Change

Massive Globalization

Nursing Informatics Leadership is Critical to Developing Cyber Resilience

Questions?

Contact information:

spoe@jhmi.edu